

BAB II TINJAUAN PUSTAKA

2.1 Studi Literatur

Studi literatur penelitian ini berfokus pada tiga penelitian sebelumnya yang dirasa relevan dengan topik yang diangkat oleh peneliti, penelitian tersebut dapat dilihat pada **Tabel 1**. analisa pada studi literatur penelitian ini menggunakan lima parameter untuk memahami serta mempelajari penelitian sebelumnya yang dijadikan rujukan, berikut penjelasan dari kelima parameter tersebut:

- a. *Contrazing*: perbandingan penelitian ini dan penelitian sebelumnya.
- b. *Comparing*: metode yang digunakan pada penelitian sebelumnya.
- c. *Critize*: kekurangan pada penelitian sebelumnya.
- d. *Synthesize*: kaitan penelitian ini dengan penelitian sebelumnya.
- e. *Summarize*: rangkuman penelitian sebelumnya.

Tabel 1. Studi Literatur

Judul Penelitian	Analisis	
<i>Purwarupa sistem pemilihan umum elektronik dengan pemanfaatan protokol Ethereum pada teknologi Blockchain[19]</i>	<i>Contrazing</i>	<i>Comparing</i>
	Penelitian sebelumnya menggunakan <i>scope</i> Pemilihan umum yang diselenggarakan pada lingkup Negara, sementara pada penelitian ini menggunakan <i>scope</i> yang terbatas pada pemilihan umum raya mahasiswa di lingkungan kampus	Metode yang digunakan adalah metode prototyping dengan teknik UAT (<i>User Acceptance Testing</i>)
	<i>Critize</i>	<i>Synthesize</i>
	Pada penelitian sebelumnya mempunyai kukarangan pada manajemen data sebesar 52% penyebabnya adalah proses eksekusi transaksi	Penerapan <i>Smart Contract</i> pada Protokol <i>Ethereum</i> digunakan pada penelitian sebelumnya digunakan sebagai referrensi pada

	yang memerlukan waktu 30 detik	Penelitian ini
	Summarize	
	<p>Penelitian ini bertujuan untuk meningkatkan keamanan sistem <i>E-Vote</i> dengan menciptakan proses yang cepat, akurat, dan transparan. Hal ini akan menjaga suara yang ada dan kerahasiaan data suara yang ditransaksikan. Smart-Contract dan Distributed System juga digunakan untuk memastikan integritas sistem <i>E-Vote</i>.</p>	
<p><i>Implementasi Teknologi Blockchain dan multi Party Computation dalam sistem E-Vote[20]</i></p>	Contrazing	Comparing
	<p>Penelitian sebelumnya menggunakan desain metode multy party computation, sedangkan pada penleitian ini menggunakan desain rancangan <i>prototype</i></p>	<p>Metode yang digunakan adalah metode prototyping dengan membangun rancangan sistem</p>
	Critize	Synthesize
	<p>Pada Penelitian sebelumnya mempunyai kekurangan pada resources dan perangkat pendukung untuk implementasi sistem secara ideal yang besar</p>	<p>Tinjauan Pustaka dan Rancangan <i>Prototype</i> sistem pada penelitian sebelumnya digunakan sebagai referensi pada penelitian ini</p>
	Summarize	
	<p>Penelitian ini memberikan solusi untuk menggunakan sistem layanan publik elektronik, seperti <i>E-Vote</i>, yang menggunakan teknik enkripsi untuk mengamankan data. Penggunaan teknologi ini melibatkan penyiaran data ke semua node dan penggunaan tanda tangan digital untuk validasi data. Sistem ini juga memungkinkan perubahan data jika data tersebut bukan dari sumber yang dapat dipercaya atau tidak dapat diandalkan.</p>	
	Contrazing	Comparing
	<p>Penelitian sebelumnya menggunakan sistem</p>	<p>Metode yang digunakan adalah studi pustaka</p>

<p><i>Implementasi teknologi Blockchain dalam aplikasi E-Vote berbasis mobile[21]</i></p>	<p><i>Blockchain</i> berbasis aplikasi mobile, sedangkan pada penelitian ini menggunakan sistem <i>Blockchain</i> dan distubuted database berbasis <i>Website</i> (localhost)</p>	<p>untuk memami lebih dalam tentang subjek dengan pendekatan metode waterfall</p>
	<p><i>Critize</i></p>	<p><i>Synthesize</i></p>
	<p>Pada penelitian sebelumnya mempunyai kekurangan pada pengembangan aplikasi pada sistem operasi smartphone yang memiliki beberapa tipe dan pembaharuan versi</p>	<p>Metode pada penelitian sebelumnya digunakan sebagai bahan referensi dalam penelitian yaitu implementasi <i>Blockchain</i> dengan metode studi pustaka menggunakan pendekatan metode waterfall</p>
	<p><i>Summarize</i></p>	
	<p>Penelitian ini berfokus pada pengembangan aplikasi <i>E-Vote</i> berbasis <i>mobile</i> yang terintegrasi dengan teknologi <i>Blockchain</i>. Tujuannya adalah mengatasi kelemahan sistem konvensional, seperti masalah keamanan yang belum memadai, risiko manipulasi, dan ketergantungan terhadap otoritas terpusat. Dengan solusi ini, diharapkan partisipasi pemilih dapat meluas melalui perangkat seluler, sekaligus meningkatkan integritas dan keamanan suara.</p>	
<p><i>Implementasi Permissioned Blockchain Berbasis Hyperledger Sebagai Penjamin Integritas Data Pada Sistem E-Vote[6]</i></p>	<p><i>Contrazing</i></p>	<p><i>Comparing</i></p>
	<p>Penelitian sebelumnya menggunakan <i>permissioned blockchain</i> dengan platform Hyperledger Fabric di mana partisipan jaringan sudah teridentifikasi, sedangkan penelitian ini menggunakan <i>public blockchain</i> berbasis Ethereum yang lebih terbuka.</p>	<p>Metode yang digunakan adalah <i>research development</i> yang meliputi tahapan studi literatur, analisis kebutuhan, perancangan arsitektur, implementasi sistem menggunakan Hyperledger, dan pengujian integritas data melalui skenario <i>insider attack</i></p>

	<i>Critize</i>	<i>Synthesize</i>
	Kekurangan pada penelitian sebelumnya adalah adanya risiko pemotongan <i>chain</i> dan kehilangan data transaksi terakhir apabila tidak ada satu pun <i>peer</i> yang memiliki <i>chain</i> yang valid , sehingga disarankan perlunya mekanisme <i>backup file chain</i> .	Tinjauan pustaka dan rancangan sistem pada penelitian sebelumnya digunakan sebagai referensi untuk memperkuat justifikasi masalah terkait integritas data , memberikan perspektif arsitektur alternatif (<i>permissioned vs public</i>), dan menjadi acuan dalam merancang skenario pengujian keamanan sistem.
	<i>Summarize</i>	
	Penelitian ini berhasil merancang sebuah sistem <i>e-vote</i> yang terintegrasi dengan <i>permissioned blockchain</i> menggunakan platform Hyperledger Fabric . Inisiatif ini bertujuan mengatasi kelemahan sistem <i>e-vote</i> konvensional yang rentan terhadap <i>insider attack</i> , dengan cara menjamin integritas data yang tersimpan di <i>server</i> . Hasil pengujian lebih lanjut menunjukkan bahwa sistem ini mampu menjaga integritas data melalui dua mekanisme utama: pemeriksaan <i>endorsement</i> untuk menolak transaksi yang mengandung perubahan salinan data, dan keputusan <i>chain</i> jika terdeteksi adanya modifikasi blok secara tidak sah	

2.2 E-Vote

E-Vote atau pemungutan suara elektronik, merupakan metode yang memanfaatkan perangkat elektronik untuk melaksanakan proses pemungutan suara dan penghitungan hasil dalam pemilihan umum[22]. Sistem *E-Vote* (pemungutan suara elektronik) merupakan sebuah metode yang melibatkan penggunaan perangkat elektronik dengan tujuan fundamental untuk meningkatkan kecepatan implementasi, menekan biaya operasional, dan mempertinggi akurasi dalam proses pemilihan[6]

2.3 Blockchain

Teknologi *Blockchain* berfungsi sebagai buku besar digital yang bersifat terdesentralisasi, di mana ia mencatat setiap transaksi pada berbagai komputer yang tergabung dalam jaringan *peer-to-peer*. Hal ini memastikan data tidak dapat diubah atau dihapus setelah tercatat, meningkatkan keamanan, dan mengurangi ketergantungan pada pihak ketiga. Teknologi ini pertama kali dikembangkan untuk mendukung Bitcoin, tetapi telah berkembang menjadi platform yang digunakan dalam berbagai aplikasi, termasuk keuangan, manajemen rantai pasokan, dan kontrak pintar[10][23]

2.4 Ethereum

Ethereum adalah platform terdesentralisasi yang menjalankan kontrak pintar, aplikasi yang berjalan persis seperti yang diprogramkan tanpa kemungkinan downtime, penipuan, atau campur tangan pihak ketiga. *Ethereum* menyediakan platform untuk aplikasi-aplikasi ini berjalan di jaringan *Blockchain*, memastikan bahwa pelaksanaan kontrak-kontrak ini ditegakkan oleh mekanisme konsensus *Blockchain* itu sendiri, bukan bergantung pada server atau otoritas terpusat[15][24].

2.5 Smart Contract

Smart Contracts adalah protokol berbasis *Blockchain* yang digunakan untuk memfasilitasi, mengeksekusi, dan menegakkan perjanjian tanpa memerlukan perantara. Kontrak ini terdiri dari kode yang berjalan secara otomatis ketika kondisi yang telah ditetapkan terpenuhi. *Ethereum* adalah platform *Blockchain* yang paling populer untuk mengembangkan *Smart Contracts*, menggunakan bahasa pemrograman seperti Solidity dan berjalan pada *Ethereum Virtual Machine* (EVM)[25].

2.6 Decentralized Applications (dApps)

Decentralized Applications (dApps) adalah aplikasi yang berjalan di atas jaringan *peer-to-peer*, seperti *Blockchain*, dan menggunakan kontrak pintar (*Smart Contracts*) untuk mengotomatisasi interaksi. Tidak seperti aplikasi tradisional yang bergantung pada server terpusat, *dApps* menawarkan transparansi dan

keamanan yang lebih tinggi melalui desentralisasi. Salah satu contoh platform populer yang digunakan untuk *dApps* adalah *Ethereum*. Pengguna *dApps* dapat berinteraksi langsung tanpa perantara, yang memberikan lebih banyak kontrol dan privasi pada pengguna[26]. *dApps* memanfaatkan arsitektur terdesentralisasi *Blockchain* untuk menghilangkan perantara, sehingga memungkinkan interaksi langsung antara pengguna sambil memastikan keamanan dan transparansi[27]

2.7 Prinsip LUBER JURDIL dalam E-Vote

Pemilu di Indonesia memiliki enam ukuran yang demokratis yakni langsung, umum, bebas, rahasia, jujur dan adil[28]. Penerapan sistem *E-Vote* di Indonesia harus mengikuti prinsip Luber Jurdil. Luber Jurdil merupakan singkatan dari Langsung, Umum, Bebas, Jujur, Rahasia. Sesuai dengan pasal UUD 1945 pasal 28C ayat 1 tentang hak mengembangkan diri sehingga penerapan sistem *E-Vote* tidak bertentangan dengan prinsip Luber Jurdil[29].

2.8 Justifikasi struktur Arsitektur dan Teknologi

Pemilihan arsitektur dan setiap komponen teknologi dalam penelitian ini didasarkan pada pertimbangan cermat untuk mencapai keseimbangan optimal antara keamanan, transparansi, privasi, dan efisiensi dalam konteks sistem *E-Vote*. Keputusan metodologis ini bertujuan untuk menjawab tantangan fundamental pada sistem pemilu elektronik konvensional, terutama terkait integritas data dan kepercayaan publik.

2.8.1 Arsitektur *Hybrid*

Dalam perancangan *Decentralized Applications (dApps)*, terdapat dua pendekatan arsitektural utama yaitu *full on-chain* dan *hybrid*. Penelitian ini mengadopsi **arsitektur *hybrid*** sebagai solusi pragmatis untuk menyeimbangkan kebutuhan yang seringkali bertentangan antara transparansi absolut dan privasi pengguna.

- a. **Komponen *On-Chain (Blockchain Ethereum)*** adalah Arsitektur yang menempatkan data pemilu sebagai data yang paling krusial, seperti rekapitulasi suara dan status sesi pemilihan, langsung di atas *blockchain*. Tujuannya adalah untuk memanfaatkan sifat dasar teknologi *blockchain* sebagai buku besar yang

tidak dapat diubah (*immutable*) dan terdistribusi. Dengan demikian, integritas hasil akhir pemilihan dapat dijamin dari risiko manipulasi, bahkan yang dilakukan oleh administrator sistem sekalipun.

- b. **Komponen *Off-Chain* (Database PostgreSQL)** Sebaliknya, adalah data identitas pemilih yang bersifat sensitif dan pribadi disimpan pada basis data konvensional. Pendekatan ini dipilih untuk melindungi privasi data pemilih sejalan dengan prinsip "Rahasia" dalam pemilu, sekaligus meningkatkan performa dan efisiensi sistem dengan mengurangi volume data yang harus diproses dan disimpan secara *on-chain* yang memerlukan biaya transaksi.

2.8.2 Teknologi *On-Chain*

Komponen *on-chain* merupakan fondasi keamanan dan integritas dari sistem yang diusulkan. Pemilihan teknologi pada lapisan ini difokuskan pada keandalan, kematangan ekosistem, dan efisiensi dalam proses pengembangan untuk memastikan logika pemilu dapat dieksekusi secara otonom dan aman.

- a. **Protokol Ethereum** dipilih sebagai platform *blockchain* karena posisinya sebagai pionir dan platform paling matang untuk pengembangan *Smart Contract*. Ekosistem Ethereum didukung oleh komunitas developer yang sangat luas dan standar teknis yang telah diadopsi secara global, menjadikannya pilihan yang andal untuk aplikasi yang menuntut keamanan tingkat tinggi seperti sistem pemilu. Kemampuan *Smart Contract* pada Ethereum untuk mengeksekusi logika secara otonom dan terverifikasi menjadi fondasi untuk menegakkan aturan pemilu secara adil dan transparan.
- b. **Jaringan Lokal (Ganache)** digunakan Untuk lingkungan pengembangan dan pengujian, penelitian ini memanfaatkan jaringan *blockchain* lokal menggunakan Ganache. Ganache dipilih karena menyediakan simulasi jaringan Ethereum yang cepat dan dapat dikonfigurasi ulang dengan mudah. Hal ini memungkinkan siklus pengembangan dan pengujian yang efisien tanpa bergantung pada latensi jaringan internet atau memerlukan biaya transaksi (*gas fee*) yang nyata, yang seringkali menjadi kendala saat menggunakan jaringan uji publik (*testnet*).

2.8.3 Teknologi *Off-Chain* dan Antarmuka Pengguna

Selain lapisan *on-chain*, komponen *off-chain* dan antarmuka pengguna memegang peranan krusial dalam mengelola data privat dan menyajikan aplikasi yang fungsional kepada pengguna. Teknologi pada lapisan ini dipilih berdasarkan pertimbangan stabilitas, kemudahan integrasi, dan kapabilitas untuk mendukung arsitektur *full-stack* yang modern.

- a. **Database PostgreSQL** dipilih sebagai sistem manajemen basis data relasional (*off-chain*) karena reputasinya yang teruji dalam hal keandalan, skalabilitas, dan kepatuhan terhadap standar SQL. Sebagai sistem *open-source* yang matang, PostgreSQL menyediakan fitur yang robust untuk mengelola data pemilih yang terstruktur secara aman dan efisien.
- b. **Framework Next.js** digunakan Untuk lapisan antarmuka pengguna dan API *backend*, penelitian ini menggunakan *framework* Next.js. Next.js dipilih karena kemampuannya dalam mendukung pengembangan *full-stack*, di mana logika *frontend* dan *backend* dapat dibangun dalam satu proyek yang terintegrasi. Pendekatan ini secara signifikan menyederhanakan proses pengembangan, memastikan komunikasi yang kohesif antara antarmuka pengguna dengan basis data *off-chain* dan *smart contract on-chain*.